

WHAT IS CLAIMED IS

1. A method for operating a device driver, comprising the steps of:
  - 1 encrypting a program code portion of a main process of a device driver;
  - 2 decrypting the encrypted program code portion in an initialization process of said device driver; and
    - 3 re-encrypting the decrypted program code portion after the decrypted program code portion is executed and before said device driver is released.
- 5 2. A method for operating a device driver, comprising the steps of:
  - 1 encrypting a program code portion of a main process of a device driver;
  - 2 initializing said device driver;
  - 3 decrypting the encrypted program code portion after the initialization process is performed;
  - 10 4 re-encrypting the decrypted program code portion after the decrypted program code portion is executed; and
    - 5 releasing said device driver after re-encrypting.
- 15 3. A method for operating a device driver, comprising the steps of:
  - 1 encrypting a program code portion of a main process of a device driver
  - 20 2 with a first encryption key and then encrypting the encrypted program code portion with a second encryption key;
    - 3 decrypting the program code portion that has been encrypted with the first encryption key with a first decryption key in an initialization process of the device driver;
    - 25 4 decrypting the program code portion that has been encrypted with the second encryption key with a second decryption key after the initialization

process is completed;

re-encrypting the program code portion with the second encryption key after the program code portion is executed; and

re-encrypting the program code portion with the first encryption key

5 after the program code portion is executed and before said device driver is released.

4. The method as claimed in claim 1, wherein at least one memory area is disposed on an application and a key for encrypting and decrypting the program code portion in said encrypting, decrypting and re-encrypting steps

10 is created corresponding to a numeric value stored in one of the memory areas.

5. The method as claimed in claim 2, wherein at least one memory area is disposed on an application and a key for encrypting and decrypting the program code portion in said encrypting, decrypting and re-encrypting steps

15 is created corresponding to a numeric value stored in one of the memory areas.

6. The method as claimed in claim 1, wherein an authentication is performed between an application and said device driver.

7. The method as claimed in claim 2, wherein an authentication is 20 performed between an application and said device driver.

8. The method as claimed in claim 1,

wherein before supplying output data to said device driver, an application detects whether or not the program code portion of said device driver has been forged and when the program code portion has been forged,

25 the application stops outputting the output data to hardware, and

wherein before supplying input data to the application, said device

driver detects whether or not the program code portion of the application has been forged and when the program code portion has been forged, said device driver stops outputting the input data to the application.

9. The method as claimed in claim 2,

5 wherein before supplying output data to said device driver, an application detects whether or not the program code portion of said device driver has been forged and when the program code portion has been forged, the application stops outputting the output data to hardware, and

wherein before supplying input data to the application, said device

10 driver detects whether or not the program code portion of the application has been forged and when the program code portion has been forged, said device driver stops outputting the input data to the application.

11. The method as claimed in claim 8,

wherein said device driver does not decrypt the encrypted data of the application, and

wherein only when the program code portion has not been forged, the application decrypts the encrypted data and outputs the decrypted data to said device driver.

12. The method as claimed in claim 9,

20 wherein said device driver does not decrypt the encrypted data of the application, and

wherein only when the program code portion has not been forged, the application decrypts the encrypted data and outputs the decrypted data to said device driver.